UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

Intellectual Ventures I, LLC, Plaintiff-Counterdefendant, v. Check Point Software Technologies, Ltd.; McAfee, Inc.; Symantec Corp.; Trend Micro Incorporated, and Trend Micro, Inc. (USA), Defendants-Counterclaimants.	Case No. 10-1067-LPS

DEFENDANTS' OPENING CLAIM CONSTRUCTION BRIEF

Collins J. Seitz, Jr. (DE Bar No. 2237)
Benjamin J. Schladweiler (DE Bar No. 4601)
SEITZ ROSS ARONSTAM & MORITZ LLP
100 S. West Street, Suite 400
Wilmington, DE 19801
(302) 576-1600
cseitz@seitzross.com
bschladweiler@seitzross.com

Attorneys for Defendant McAfee Inc.

Jack B. Blumenfeld (DE Bar No. 1014)
Thomas C. Grimm (DE Bar No. 1098)
MORRIS, NICHOLS, ARSHT & TUNNELL LLP
1201 North Market Street
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
tgrimm@mnat.com

Attorneys for Defendants Check Point Software Technologies Inc. and Check Point Software Technologies Ltd. and Symantec Corporation

Karen Jacobs Louden (Bar No. 2881)
Michael J. Flynn (Bar No. 5333)
Morris, Nichols, Arsht & Tunnell LLP
1201 North Market Street
Wilmington, DE 19899
(302) 658-9200
klouden@mnat.com
mflynn@mnat.com

Attorneys for Defendants Trend Micro Incorporated and Trend Micro, Inc. (USA)

DATED: JUNE 5, 2012

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

OTHER AUTHORITIES

I. INTRODUCTION AND SUMMARY

This is a patent lawsuit. Defendants are four innovation-based companies: Check Point Software Technologies; McAfee, Inc.; Symantec Corp.; and Trend Micro. Each is a leader in its field and has sold advanced computer security products and services for many years. Plaintiff, Intellectual Ventures LLC I ("IV"), has never provided any computer security products or services and thus does not compete in the market for those products or services. It obtained title to the four asserted patents on one day and filed this lawsuit on the next. The four patents claim certain methods and systems for managing and protecting against viruses and spam.

A consistent theme pervades IV's proposed constructions for its recently acquired patents. IV seeks to re-write in this litigation the claims that were granted during prosecution. It does so because it requires the asserted claims to have broad meanings so IV can assert them against these four defendants, whose products and services are different from each other's. A disputed phrase from U.S. Patent No. 7,506,155 ("converting the executable code from an executable format to a non-executable format") highlights the tact that IV has repeatedly taken with its proposals. The '155 patent criticizes computer security products that "arbitrarily delete or withhold e-mail content without specific knowledge and authorization of the owner of the e-mail system." *Id*. 3:6-9. The patent's narrow solution was to "convert[] all data received via e-mail (mail and attachments) to non-executable" format, *id*. 2:24-25, so that a recipient could still receive the e-mail, but it would no longer pose a threat.

IV, the current patent owner, now proposes to revise this disputed limitation to mean "rendering executable code inoperable." IV's proposal has three telling defects. First, it would encompass deleting code, thus eviscerating a later limitation that requires "forwarding the non-executable format to a recipient of the e-mail message." Code that has been deleted cannot be forwarded. Second, the limitation, on its face, requires conversion, not deletion. Executable code that has been converted into a different format (for example, into a PDF format) is still present, just not in an executable format—the conversion renders it unable to open processes or applications. That is the defining feature of code in "executable" format: it can open processes

or applications. Third, it strays back into the very territory that the patent criticized. Deleting code without the user's knowledge presumes that the code is a virus. But as noted the patent teaches that "software systems, including security programs, should not arbitrarily delete or withhold e-mail content without specific knowledge and authorization of the owner of the e-mail system." *Id*. 3:6-9. IV's litigation-driven proposal construction would do exactly what the patent criticizes.

IV's constructions neither stay true to the granted claim language nor most naturally align with each patent's description of each invention. Defendant's, in sharp contrast, do both, and it would be appropriate to adopt them.

II. FACTS

IV asserts four unrelated patents. None share a common specification or named inventors. U.S. Patent No. 7,506,155, entitled "E-mail virus protection system and method," claims priority to June 2000 and issued in March 2009. U.S Patent No. 6,460,050, entitled "Distributed content identification system," was filed in December 1999 and issued in October 2002. The patent entitled "Automated post office based rule analysis of e-mail messages and other data objects for controlled distribution in network environments," U.S. Patent No. 6,073,142, was filed in June 1997 and issued in June 2000. Finally, the "telephone network" patent, U.S. Patent No. 5,987,610, was filed in February 1998 and issued in November 1999.

As the Court directed, a DVD tutorial on the technology at issue in this case is being filed herewith. For the Court's convenience, Appendix A is a textual version of that tutorial.

III. DISCUSSION

IV's claim construction positions disregard a number of core claim construction principles. First, the claim language itself—both the disputed language and the context of its surrounding words—provides substantial guidance. Second, the patent's specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term. In particular, descriptions of "the present invention" receive great weight. Ultimately, the interpretation to be given a term can only be determined

and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. Third, the construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction. This Court has recognized these core principles in its own jurisprudence, *e.g.*, *Xerox Corp. v. Google, Inc.*, 801 F. Supp. 2d 293, 297-98 (D. Del. 2011), which accord with Supreme Court and Federal Circuit jurisprudence. They cannot be disregarded, as IV's proposals would require. When followed, they lead to defendants' constructions.

A. The '155 Patent

This patent is directed to protecting computer networks against viruses. JC Ex. B, '155 Col.1:18-24, which are a form of executable code. *Id.* 1:29-32.[1] According to the patent, the prior art methods were "only marginally successful," because they "attempt[ed] to identify the existence of a virus before taking steps to protect a user," *id.* 3:43-47, *i.e.*, the prior art methods allowed the executable code to run before protecting against it. Under the patent's methods, a "host computer converts ***all*** data received via e-mail (mail and attachments) to non-executable" format," *id.* 2:23-25, which "by nature" cannot open applications or processes. *Id.* 2:18-23. All of the data is converted because "[r]ecipients of e-mails are ultimately more qualified to determine what information is acceptable than a generalized software program or system." *Id.* 2:62-64; *see also id.* 3:5-9 (software should not decide what is deleted).

IV asserts claims 2-4, all of which depend from claim 1. The parties present four disputed phrases for construction.

i. "Converting the executable code . . . ." means converting, not deleting

In the '155 patent, "executable code" is code that exists in a format that can open applications or processes. JC Ex. B, '155 Col. 2:16-23. Indeed, that is "executable" code's defining feature: it exists in a format that can be run. JC Ex. H, *Microsoft Press Computer*

[1] The parties' Joint Claim Construction Chart Exhibits ("JC Ex.") are attached to *Notice of Filing of Parties' Joint Claim Construction Chart* (D.I. 214). Unless noted otherwise, all emphasis herein has been supplied, and all internal quotations in citations omitted.

Dictionary, 182 (3d ed. 1997) ("executable" means "a program that can be run") (hereafter "*Microsoft Dictionary*"). An "executable" program is one that exists "in a format that can be loaded into memory and run by a computer's processor." *Id*. at 182 (defining "executable program"). For example, otherwise executable code that exists in PDF format cannot cause a computer to open applications or processes, precisely because it exists in the PDF format.

The disputed limitation is directed to converting code, and in particular to converting it from one format (executable) to another (non-executable); the conversion from one format to the other prevents the code from opening applications or processes, thereby allowing (as the claim later requires) "forwarding the non-executable format to a recipient of the e-mail message":

Disputed Claim Phrase	**Defendants' Construction**	**IV's Construction**
"converting the executable code from an executable format to a non-executable format"	"transforming the executable code into a copy that cannot open any processes or applications"	"rendering the executable code inoperable"

The disputed claim language itself, which guides claim construction, *e.g.*, *Phillips v. AWH Corp*., 415 F.3d 1303, 1314 (Fed. Cir. 2005) (*en banc*), rejects IV's overbroad construction. That claim language requires "***converting*** the executable code . . . to a non-executable format." Thus, the executable code is transformed into a different format—one unable—one unable to open processes or applications—but the code still exists. Hence defendants' construction: "transforming the executable code into a copy that cannot open any processes or applications." IV's proposal, by contrast, would change the claim also to encompass deleting the code rather than converting it.

The surrounding claim language points the same way. Claim language must be construed in the context of the surrounding limitations, not in isolation. *IGT v. Bally Gaming Int'l, Inc*., 659 F.3d 1109, 1116-17 (Fed. Cir. 2011). Here, the claim's final limitation requires "forwarding the non-executable format to a recipient of the e-mail message." JC Ex. B, '155 Col. 6:36-37. Simply deleting code would leave nothing to forward. Likewise, the claim's second limitation further requires that, notwithstanding the conversion process, in the new format the executable code must, as part of the e-mail message after conversion, "retain[] an appearance, human

readability, and semantic content of the e-mail message" before conversion. *Id.* 6:34-35. Simply deleting code retains none of those.

Ordinary artisans' normal usage of these claim terms at the time confirms this construction. The patent cites the *Microsoft Dictionary* as an "Other Reference." It is thus intrinsic evidence. *E.g.*, *Phillips*, 415 F.3d at 1317 (intrinsic evidence "includes the prior art cited during the examination of the patent."). The ordinary understanding of the related term "conversion" to mean "[t]he process of changing from one form or format to another; where information is concerned, a changeover that affects form but not substance," JC Ex. H, *Microsoft Dictionary* at 188-189, and an "executable" program as one that exists "in a format that can be loaded into memory and run by a computer's processor," *id*. at 182. In the claims, the substance of the executable code is maintained, because it is copied into a different format; but the format is changed, from executable to non-executable. A construction that would allow for the deletion of the executable code is not consistent with the claim language nor the ordinary artisan's knowledge.

IV's proposal would also conflict with the specification's description of the invention. As the Federal Circuit emphasized *en banc* in *Phillips*, claims must be read in view of the specification, of which they are a part; hence, the "specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Phillips*, 415 F.3d at 1315 (citation omitted). The specification's weight "has a long pedigree in Supreme Court decisions." *Id*. (citing six Supreme Court cases). In particular, the specification's description of "the present invention" receives great weight and can be dispositive in claim construction. "When a patent thus describes the features of 'the present invention' as a whole, this description limits the scope of the invention," *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1308 (Fed. Cir. 2007), because "[t]he public is entitled to take the patentee at his word" that the "present invention" defines claim scope. *Honeywell Int'l, Inc. v. ITT Indus., Inc.*, 452 F.3d 1312, 1318 (Fed. Cir. 2006).

Here, the specification states that "[t]he present invention" requires "passing all e-mail and attachments through various conversion states that, while harmless to e-mail text and attachments, the conversions are lethal to executable code (viruses)." JC Ex. B, '155 Col. 2:26-30. As the Summary of the Invention explains, "if a host computer converts ***all data*** received via e-mail (mail and attachments) to non-executable entities, any embedded virus is rendered inoperable," *id*. 2:23-26 (emphasis added), because "[n]on-executable entities are, by nature, incapable of launching a virus," *id*. 2:22-23. Thus, consistent with the claims and the ordinary artisan's understanding, the specification explains that "[a]ny executable programs or other suspicious parts of incoming e-mail messages are . . . converted to non-executable format such as Adobe Acrobat PDF[.]" *Id.* Abstract. Not deleted, as IV's proposal would encompass. Converted from one format to another, as in defendants' construction.

ii. "Retains an appearance, . . . and semantic content": "substantially all" is not enough

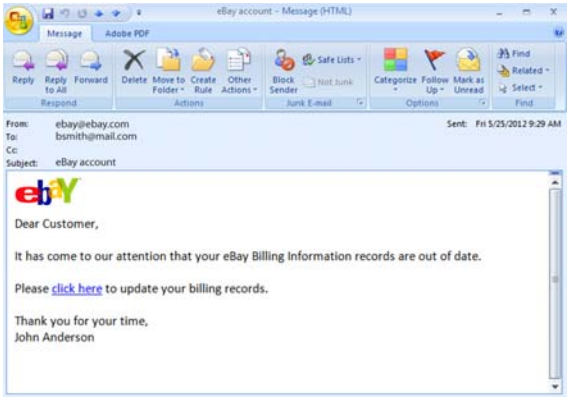
As just explained, this claim contemplates a conversion process from one format to another. Like the just-discussed claim phrase, this disputed claim phrase confirms that the conversion process does not change what the user sees. The parties' dispute is:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"retains an appearance, human readability, and semantic content of the e-mail message"	"keeps the visual display, human readability, and meaning of the e-mail"	"retains substantially the same appearance, human readability, and semantic content of the e-mail message, such that all or substantially all alphanumeric text in the e-mail message remains human readable"

The claim language supports defendants' construction. The disputed limitation begins with "retains." In ordinary usage, "retain" means "to keep." Winters Ex. 1, *Webster's Ninth New Collegiate Dictionary* at 1006 (Merriam-Webster 1986) ("*Webster's*").[2] This limitation

[2] Evidence not included in the JC is attached to the Declaration of Vernon M. Winters, submitted herewith. The Federal Circuit has specifically relied on *Webster's*. *E.g.*, *Liquid Dynamics Corp. v. Vaughan Co.*, 449 F.3d 1209, 1217 n.1 (Fed. Cir. 2006) (assessing the scope of "toroidal").

requires keeping the "appearance, human readability, and semantic content of the e-mail message." When a person is viewing something, in normal usage that thing's "appearance" is its visual display. The ordinary understanding of "semantic content" is "meaning," both in English, *see* Winters Ex. 1, *Webster's* at 1068, and in the computing context, JC Ex. H, *Microsoft Dictionary* at 428. (The parties agree that the meaning of "human readability" is clear.) In ordinary usage the disputed phrase means "keeps the visual display, human readability, and meaning of the e-mail."



Consider the parties' respective constructions in the context of an example. Suppose a person sends another an e-mail message that looks like this the picture to the left. Under defendants' construction, that is also what the recipient sees (although the hyperlink would no longer open to a potentially malicious web address). The converted e-mail message retains an appearance, human readability, and semantic content—but the executable code is in a non-executable format, as the prior limitation requires. Thus, the recipient still sees an underlined blue link that looks like a hyperlink, but that is not able to open any applications or processes, *i.e.*, it is not able to run.

But under IV's proposal, that is not necessarily what the user would see. IV proposes to change and in particular to broaden the claim language to mean "retains ***substantially the same appearance***, . . . , such that all or ***substantially all alphanumeric text*** in the e-mail message remains." Substantially the same or substantially all, measured by what standards? From whose perspective? The sender's or the recipient's—and why that person's perspective, rather than the other's? What if those two perspectives conflict? Does keeping 95% of the e-mail message suffice? How about 65%? "The scope of claim language cannot depend solely on the unrestrained, subjective opinion of a particular individual purportedly practicing the invention." *Datamatize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1350 (Fed. Cir. 2005).

The Summary of the Invention likewise supports defendants' construction. It specifies a process that "***converts all data*** received via e-mail (mail and attachments) to non-executable entities," and states that "the present invention describes a method and system of virus protection that involves passing ***all e-mail*** and attachments through various conversion states that, while ***harmless to e-mail text and attachments***, the conversions are lethal to executable code (viruses)." JC Ex. B, '155 2:23-30. The Summary of the Invention thus rejects the notion of keeping only "substantially all" of the e-mail message or "substantially all alphanumeric text." Such statements delineate the invention as a whole, not just a preferred embodiment, and the law gives them extra weight. *See Verizon Servs.*, 503 F.3d at 1308.

The prosecution history's guidance aligns with the claims and the specification. During the parent application's prosecution, which is relevant for claim construction purposes, *Hakim v. Cannon Avent Group, PLC*, 479 F.3d 1313, 1317-18 (Fed. Cir. 2007), the patent office rejected claims with this limitation because of Kellum, U.S. Patent No. 6,487,664. *See, e.g.*, JC Ex. G, '155 Parent FH, 08/12/03 Amendment at 10-15. The ultimately successful applicants argued that in their claimed invention, "the recipient of the e-mail message is . . . ***able to see***, in a timely fashion, ***any human-readable content*** for which the e-mail message was sent in the first place," *id.*, 03/07/03 Amendment at 5, and that "the application-level conversion of the present invention ***retains the original human-readable semantic content***," *id.*, 08/12/03 Amendment at 12. Not "substantially the same appearance" or "substantially all alphanumeric text," as the current patent owner, IV, argues. These statements inform claim scope, *800 Adept, Inc. v. Murex Securities, Ltd.*, 539 F.3d 1354, 1364-65 (Fed. Cir. 2008), and point away from IV's litigation construction. A patent owner cannot change in litigation the scope that the applicant urged when trying to avoid prior art during prosecution. *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1349-50 (Fed. Cir.), *cert. denied*, 125 U.S. 821 (2004).

Finally, in a defect that IV's other proposals repeat, IV's "construction" of this phrase simply parrots back the claim language at issue and then adds various qualifications. As this Court has observed, the law frowns on defining a phrase by repeating it. *Eppendorf AG v.*

Nanospher, Inc., No. 09-0504, slip op. at 14 (D. Del. Jul. 12, 2010) (criticizing and rejecting proposed construction because it "repeats the words [of the claim] themselves.").

iii. "Forwarding the non-executable format"

Notwithstanding that IV (1) will not agree to defendants' construction, (2) will not specify what "ordinary meaning" means, and (3) agrees that the Court should construe a phrase containing the disputed language "executable format," IV argues that this disputed limitation is within the common understanding of laypeople and thus need not be construed. When the parties dispute a limitation, construction is warranted. *02 Micro Int'l Ltd. v. Beyond Innovation Tech. Co*., 521 F.3d 1351, 1361 (Fed. Cir. 2008). The parties' dispute is:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"forwarding the non-executable format"	"sending to a new recipient the copy that cannot open any processes or applications"	"plain and ordinary meaning"

Both the claim language and the specification support defendants' construction, which requires that the non-executable copy created by the conversion process, described above, be sent onwards to the recipient. "Forwarding" ordinarily means "to help onward, to send forward," Winters Ex. 1, *Webster's* at 485, and the Abstract confirms that the result of the conversion process is "sent to the recipient." JC Ex. B, '155 Abstract. As discussed above, converting formats eliminates all executable code by a process that will "create a readable copy" of the code, "but [] not allow the attachment to open any processes or applications." *Id.* 3:60-63. Thus, in this construction, the non-executable copy created during conversion is sent to the recipient.

Defendants' construction is also consistent with other descriptions in the specification. For example, the specification describes how, in the context of converting macros, the non-executable format is forwarded once it has been created: "If the execution of the macro was necessary to produce the information contained in the tested documents, then the macro's contribution is contained in the print image copy of the document produced by the sacrificial PC when it executed the document with macros disabled. This is the copy sent to the recipient." *Id.* 5:31-36. Thus, the conversion process creates a harmless copy—one that cannot open processes

or applications—which is sent to the recipient.

iv. "Deactivating the hypertext link"

Claim 3 depends from claim 1. Subject to the appropriate construction claim 1's other disputed limitations, based on the claim language and the specification's description of "the invention," "deactivating the hypertext link" simply means "rendering the hypertext link inoperable." That is precisely the Summary of the Invention's description of how the invention converts executable virus code generally: "Therefore, if a host computer converts all data received via e-mail (mail and attachments) to non-executable entities, ***any embedded virus is rendered inoperable***." JC Ex. B, '155-2:23-26. The parties' dispute is:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"deactivating the hypertext link"	"rendering the hypertext link inoperable"	"rendering the hypertext link inoperable as an executable link to the specified URL, while leaving alphanumeric text that is identifiable as a hypertext link"

As just noted, defendants' construction hews closely to the specification. *Id*. 2:23-26; *see also id*. 3:41-43. Because the law gives particular weight to a patent's Summary of the Invention, *Verizon Servs.*, 503 F.3d at 1308, defendant's construction is correct.

In contrast, IV's proposal leaves the meaning of this claim term muddled. What does "the specified URL" mean? The specification does not contain that phrase. Does it mean the URL to which the hyperlink apparently redirects? Or does it mean the URL to which the hyperlink actually redirects? That different can be crucial: redirecting to a different URL can be what makes a hyperlink malicious. And what does "leaving alphanumeric text" mean? All of the alphanumeric text? Only some? If only some, what is the dividing line? "The scope of claim language cannot depend solely on the unrestrained, subjective opinion of a particular individual purportedly practicing the invention." *Datamatize, LLC*, 417 F.3d at 1350. IV's proposal creates confusion, which is contrary to the purpose of claim construction. *Funai Elec. Co., Ltd. v. Daewoo Elecs. Corp.*, 616 F.3d 1357, 1366 (Fed. Cir. 2010).

B. The '050 Patent

The '050 patent is directed to filtering e-mail messages and in particular spam and viruses. Prior art systems that involved remote review (either automatically or by people) of e-mail messages had three problems. First, they took up too much network bandwidth: in addition to the initial delivery, the message had to be sent to the remote location and then transmitted back. JC Ex. C, '050 1:49-56. Second, confidentiality issues arose if people performed the review. *Id*. 1:44-48. Third, spammers and other senders of unwanted e-mail were becoming increasing sophisticated in avoiding automated detection. *Id*. 1:56-64. The patent purported to solve these problems with methods and systems that involved "generating a digital identifier" for the e-mail message, forwarding that identifier (instead of the whole message) to a processing system, and then processing that e-mail based on whether it matched a characteristic of other digital identifiers that represented other e-mail message. *Id*. 2:38-43.

IV asserts seven claims: independent claims 9, 16, and 22, and dependent claims 13, 15, 20, and 24. The parties present seven disputed terms or groups of them.

i. Indicating or identifying the presence or absence of a characteristic

Using slightly different language, each of the independent claims contain a core requirement: that the presence or absence of a "characteristic" be identified or indicated. This language is best read in context, because disputed claim language must be construed in the context of the surrounding limitations in which they arise, not in isolation. *IGT*, 659 F.3d at 1116-17. Claim 16, for example, is directed to "[a] method of filtering an e-mail message" that specifies a series of steps. Its first limitation requires "receiving, . . . a digital content identifier created using a mathematical algorithm unique to the message content[.]" JC Ex. C, '050 8:46-48. The second limitation requires comparing that unique digital content identifier "to determine whether the message has ***a*** characteristic." *Id.* 8:51-55. The disputed third limitation requires "responding to ***a*** query . . . to identify the existence or absence of ***said*** characteristic[.]" *Id*. 8:56-59. In other words, after receiving the identifier, the second limitation's step determines whether an e-mail message has a property (*e.g.*, whether it is spam) and the disputed third limitation's

step responds, in a binary way, to a query about whether that property is present (*e.g.*, is this spam? is this a virus?). In essence, the disputed third limitation provides the result of a true/false test for the existence or absence of the property that was the subject of the query.

Each of these disputed limitations share in common the indication or identification of: the presence or absence of "***a*** characteristic" (claim 22), "***the*** characteristic" (claim 9), or "***said*** characteristic" (claim 16). That language reflects the true/false result of a query: is a property—that is, a characteristic—present or not? The disputes are:

Disputed Claim Phrases	**Defendants' Construction**	**IV's Construction**
"an indication of the characteristic" (claim 9)	"the result of a true/false test for a property of the content"	"a descriptor of the content (e.g., spam, virus, junk e-mail, copyrighted)"
"identify the existence or absence of said characteristic" (claim 16)	"provide the result of a true/false test for the existence or absence of the property of the content"	"identify whether or not the message is of a certain type or classification"
"indicating the presence or absence of a characteristic" (claim 22)	"providing the result of a true/false test for the presence or absence of a property of the content"	"indicating the presence or absence of a characteristic (e.g., spam, virus, copyright, bulk e-mail)"

As just explained, the claim language points towards defendants' constructions. So does the specification. It states that in "[t]he present invention," identifying a characteristic about an e-mail message involves providing the result of a true/false test about content: "the digital identifier is forwarded to a processing system which correlates any number of other identifiers through a processing algorithm to determine whether ***a*** particular characteristic for the content exists. ***In essence, the classification is a true/false test for the content based on the query for which the classification is sought***." JC Ex. C, '050 Col. 3:11-16. In the next sentence, the specification gives examples of this classification based on a true/false test of the content: "For example, a system can identify whether a piece of e-mail is or is not spam, or whether the content in a particular file matches a given criteria indicating it is or is not copyrighted material or contains or does not contain a virus." *Id*. 3:16-20. Likewise, that in "the present invention," the classification is based on a true/false test of the content: the "system . . . includes a database and processor which determines, based on an algorithm which varies with the characteristic

tested, whether the e-mail meets the classification of the query (e.g., is it spam or not?)." *Id*. 3:46-49. Finally, the Abstract explained the invention as "include[ing] a characteristic comparison routine ***identifying the file as having a characteristic*** based on ID appearance in the appearance database." The law accords special emphasis to specification descriptions of "the present invention." *Verizon Servs.*, 503 F.3d at 1308.

IV's attempts here to evade the clear teachings of the specification are like those the Federal Circuit rejected in *Decisioning.com*, 527 F.3d at 1307-10. There, as here, the dispute involved a claim phrase that, read in isolation, might encompass the patentee's construction. There, the issue was whether "remote interface" meant "kiosk" or could include a user's personal computer in claims directed to automated loan processing. In argument like plaintiff's, the patentee there argued that the claim language was broad because it did not on its face exclude certain coverage. *Id*. at 1307. The court acknowledged that "[d]ivorced from the specification," the disputed phrase "remote interface" could encompass a consumer-owned personal computer. But the patent stated that "the present invention is the closed loop performance of financial functions via a computer and monitor mounted in a kiosk," *id*. at 1310, so the court rejected the patentee's divorced-from-context construction. That would be appropriate here, too.

IV's proposed constructions suffer from additional defects. Its proposed construction for the phrase from claim 9 replaces "indication of the characteristic" with "descriptor," a word that appears nowhere in the specification or claims of the patent and introduces a new concept that is not part of the claim language. Its proposed construction for the disputed limitation from claim 22 does nothing but repeat the claim language and then add additional qualifications to them, an approach frowned upon in the law of this court. *Eppendorf*, slip op. at 14.

ii. The "matching" limitation

Claim 9's second limitation requires determining whether there is a match between (a) each received content identifier and (b) a characteristic of other identifiers. Claim 9's third limitation then uses that matching to "output[] . . . an indication of the characteristic of the data file based on" the matching step. Hence defendants' construction. The parties' dispute is:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"determining . . . whether each received content identifier matches a characteristic of other identifiers" (claim 9)	"matching a content identifier to a characteristic of other identifiers"	"determining . . . whether each received content identifier has the same characteristic as other content identifiers"

The disputed claim language, which must be assessed in the context of the surrounding limitations, *IGT*, 659 F.3d at 1116-17, points to defendants' construction. Claim 9 is directed to "[a] method for identifying characteristics of data files." JC Ex. C, '050 Col. 8:13-14. In the first step of the claimed method, the processing system receives file content identifiers for data files. *Id*. 8:15-16. In the second step, the processing system matches a file content identifier to a characteristic of other file content identifiers. *Id*. 8:20-22. In the third step, the processing system outputs, in response to a request, "an indication of the characteristic of the data file based on said step of determining," *id*. 8:23-26—*i.e.*, indicating whether there is a match for the result of that algorithm. In that context, the most natural reading of the disputed second limitation is that it means "matching a content identifier to a characteristic of other identifiers."

The specification confirms defendants' construction. The Summary of the Invention, to which the law ascribes great weight, *Verizon Servs.*, 503 F.3d at 1308, reminds that "***the invention*** comprises a method for identifying a characteristic of a data file. The method comprises the steps of: generating a digital identifier for the data file and forwarding the identifier to a processing system; ***determining whether the forwarded identifier matches a characteristic of other identifiers***; and processing the e-mail based on said step of determination." JC Ex. C, '050 Col. 2:37-43. In a column beginning "[t]he present invention," the specification likewise informs that "the digital identifier is forwarded to a processing system which correlates any number of other identifiers through a processing algorithm to determine whether a particular characteristic for the content exists. . . . For example, a system can identify whether a piece of e-mail is or is not spam, or ***whether the content in a particular file matches a given criteria*** indicating it is or is not copyrighted material or contains or does not contain a virus." *Id.* 3:7-20. The Abstract corroborates this construction: "[t]he system includes . . . a method for identifying a characteristic of a data file comprises the steps of: generating a digital

identifier for the data file and forwarding the identifier to a processing system; ***determining whether the forwarded identifier matches a characteristic of other identifiers***; and processing the data file based on said step of determination." *Id.* Abstract. Other specification disclosures are the same effect. *Id*. 6:5-10 (content identifier matches to a characteristic of other identifiers).

Defendants' construction stays true to the claim language and most naturally aligns with the patent's description of the invention. *Phillips*, 415 F.3d at 1315 (such a construction is correct). IV's, by contrast, deletes the "matching" requirement from the claims, when both the claim language and the specification require it. "A patentee may not proffer an interpretation for the purposes of litigation that would alter the indisputable public record consisting of the claims, the specification . . . , and treat the claims as a 'nose of wax.'" *Southwall Tech., Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1578 (Fed. Cir. 1995).

iii. "Data file[s]"

Asserted claim 9, and its dependent claims 13 and 15, are directed to a "method for identifying characteristics of data files." The parties disagree as follows:

Disputed Claim Phrases	Defendants' Construction	IV's Construction
"data file[s]"	"a collection of information presented as a unit to a user"	"IV has determined that no construction is needed for this term and withdraws its election. Otherwise, plain and ordinary meaning. Otherwise, "'any type of text or binary data.'"

The claim text confirms defendants' construction. Independent claim 9's last limitation requires "an indication of the characteristic of the data file . . . ." JC Ex. C, '050 Col. 8:25-27. Likewise, unasserted claim 25 requires "characterizing the data file . . ." *Id.* 10:18. That language strongly implies that the "data file" must be considered as a unit; otherwise, it could not have a single characteristic, *i.e.*, "the characteristic." Dependent claim 13 requires that the "data file" be an e-mail message, *id*. 8:34-35, and the patent treats an e-mail message as the entirety of the message, including attachments. *Id*. 1:49-50. The ordinary artisans' usage of "file" also points towards defendants' construction. The ordinary artisan considered a "file" to be "[a]

complete, named collection of information, such as a program, a set of data used by a program, or a user-created document"; it was the "'glue that binds a conglomeration of instructions, numbers, or words into a coherent unit that a user can retrieve, change, delete, save, or send to an output device." *Microsoft Dictionary* at 194.

IV's proposal, by sharp contrast, offers no such coherence. Under its amorphous proposal, a "data file" simply means "any type of text or binary data," thereby deleting the explicit requirement that the data have a further characteristic: that it not just be data, but that it be a "data file." IV's proposal is effectively limited to defining "data." *See id.* at 129 ("data" means "an item of information"). IV's proposal effectively deletes "file" from this limitation, and thus cannot be right.

iv. "File [digital] content identifier [ID]"

All of the claims require a "file content identifier" or "digital content identifier" to be "created . . . using a mathematical algorithm" that corresponds to a data file or an e-mail message. JC Ex. C, '050 Cols. 8:15-19, 8:46-48 & 9:20-22. The parties' dispute is:

Disputed Claim Phrases	Defendants' Construction	IV's Construction
"file content identifier" "file content ID" "digital content identifier" "digital content ID"	"an identifier for the contents of a file [or digital content], that is not a portion or portions of the content"	"a digital identifier reflecting at least a portion of the content of a data file"

IV's construction is overbroad. Under it, a "file content identifier" could consist of any of (1) some excised part of the e-mail message such the "subject" line of an e-mail, (2) a hash of less than the entire file, or (3) a hash of the file as a whole. IV's first position conflicts with the claim language on its face. Each of these claims requires that the identifier be "***created*** . . . using a mathematical algorithm." An identifier that consists merely of some excised portion of the e-mail message would not have been "created" but instead would have been, for example, "filtered" from the file being identified. And each of IV's positions conflicts with the prosecution history. During prosecution, the claims were rejected based on prior art that simply used a portion of the email message (for example, the subject line) to filter the message, JC Ex. J,

'050 FH, 02/20/02 Response B and Amendment at 10, because the examiner considered such a portion to be a digital content ID, *id.* at 10-11. But the applicants expressly represented that, in its invention, such portions were not not file content IDs or digital content IDs, arguing that "it is clear that ***a 'file content ID' is not the same as*** the simple filtering of ***portions of the email***. . . . such ID must be separate and apart from the file itself," *id.* at 11, and that the reference "simply teaches examining ***portions of an email message, not computing a file content identifier***." *Id.* at 15. As the applicant stated, its invention was different because the prior art "does not attempt to modify or 'hash' the data before it performs its processing." *Id.*

Whether viewed to inform claim construction, *Hakim*, 479 F.3d at 1317-18, or under the separate doctrine of prosecution disclaimer, *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003), based on these clear, unequivocal statements, the current patent owner cannot obtain the different claim scope it now seeks in litigation.

v. The "file content identifier generator agent(s)" claims

In claim 9 and its dependent claims 13 and 15, the file content identifiers are created by a plurality of "file content identifier generator agents." JC Ex. C, '050 Col. 8:15-19. The parties agree that these file content identifier generator agents are software running on a computer and that they create file content identifiers. (This is what the claim language requires: that there be "agents" that "generate" file content identifiers.) IV, however, proposes to change the claim language to add two additional requirements, namely that the agents also (1) transmit the file content identifiers (2) "to a second tier system." The parties' dispute is:

Disputed Claim Phrases	Defendants' Construction	IV's Construction
"file content identifier generator agent(s)"	"software running on a computer that creates file content identifiers"	"software running on a computer that creates and transmits file content identifiers to a second tier system"

There is no support for IV's proposed additions to claim 9's language. The claim never mentions a "second tier system" and certainly never mentions that the file content identifier generator agents "transmit" the file content identifiers to such a system. Rather, the claim

requires—and requires only—that the file content identifiers be received by "a processing system." JC Ex. C, '050 Col. 8:15. IV's position imposes the additional requirement that this "processing system" be a "second tier system," but in certain preferred embodiments, the "third tier" system, *id.*, Fig. 3, 5:31-35, not the second tier system, receives file content identifiers. IV's construction excludes preferred embodiments. Absent an express disclaimer in the specification or prosecution history, such a construction is not correct. *E.g.*, *Oatey Co. v. IPS CORP.*, 514 F. 3d 1271, 1276-1277 (Fed. Cir. 2008).

An even more fundamental problem with IV's proposed construction is that it replaces a phrase that has a clear meaning with a definition that contains an unclear and undefined term that exists nowhere in the claims as written: "second tier system." The purpose of claim construction is clarify the meaning of the claims and facilitate the proper understanding of the claims, not to introduce new ambiguous terms. *See*, *e.g.*, *Funai Elec. Co., Ltd. v. Daewoo Elecs. Corp.*, 616 F.3d 1357, 1366 (Fed. Cir. 2010) (the criterion for proper claim construction "is whether the explanation aids the court and the jury in understanding the term as it is used in the claimed invention"). Although the specification refers to "first tier," "second tier," and "third tier," it never explains what constitutes a "tier" or how they should be counted. *See* JC Ex. C, '050 Figs. 2 and 3. Moreover, the specification makes certain statements about what a "second tier system" is or contains. For example, referring to the "second tier system" of the embodiment in Figure 2 of the patent, the specification states that "[s]econd tier system 30 includes a database and a processor." *Id.* 3:46-47. Importing the "second tier system" language from a preferred embodiment into the claims also invites the jury to import the structure making up the second tier system in that embodiment into the claims. Since the language of claim 9 does not require a database, it would be incorrect to import such a limitation into the claim by way of IV's proposed "second tier system" construction.

IV's added requirement is unnecessary, lacks support in the language of the claims, and risks misleading and confusing the jury. In contrast, defendants' proposed construction is clear,

matches the plain meaning of the claim language, and is fully consistent with the intrinsic evidence. For these reasons, defendants' proposed construction is the correct one.

vi. "Digital content identifier . . . unique to the message content": "unique" does not merely mean "particular"

Claim 16 and its dependent claims require a "digital content identifier created using a mathematical algorithm unique to the message content." The parties agree that "unique to the message content" modifies "digital content identifier" rather than "mathematical algorithm." Where they disagree is principally in whether the digital content identifier must actually be "unique" as specified in the claim or merely "particular" as IV now proposes. (IV also replaces the claim phrase "digital content identifier" with "file content identifier.") Hence:

Disputed Claim Phrases	Defendants' Construction	IV's Construction
"digital content identifier created using a mathematical algorithm unique to the message content"	"digital content identifier created using a mathematical algorithm never corresponds to more than one message content"	"a file content identifier (defined above) created using a mathematical algorithm; the identifier being particular to the message content"

In ordinary usage, "unique" means "being the only one : sole." *E.g.*, Winters Ex. 1, *Webster's* at 1290. By requiring that the identifier be "unique to the message content," this limitation requires that the message content in question be the only message content that has that identifier. An identifier would not be "unique" if it corresponded to two different messages. But IV's proposal replaces the well-understood and precise word "unique" with the ambiguously broader word "particular." The principal meaning of "particular" is "of, ***relating to***, or being a single person or thing." *See, e.g., id.* at 858. IV thus rewrites the claim: "~~digital~~ file content identifier created using a mathematical algorithm ~~unique~~ particular to, i.e., relating to the message content." But the applicant knew how and when to use "particular"; two other claims (22 and 25) use that term, suggesting that "unique" means something different. *Invitrogen Corp. v. Clontech Labs., Inc.*, 429 F.3d 1052, 1078 (Fed. Cir. 2005).

Notwithstanding the common usage of "particular," it may be that IV intends it to be coterminous with "unique"—to mean the same thing, and nothing more. If that is true, IV

should not resist defendants' construction, and in any event, defendants' clearer and more explicit construction is superior, *Funai*, 616 F.3d at 1366, even leaving aside that it stays faithful to the claim language.

vii. "Characterizing the files . . ."

Claim 22 requires as a step in its method this phrase. The parties' dispute is:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"characterizing the files on the server system based on said digital content identifiers received relative to other digital identifiers collected in the database"	"classifying with a true/false test the files on the server system by comparing said digital content identifiers with other digital identifiers collected in the database"	"classifying the files on the server system by comparing them to other digital identifiers collected in the database"

There are two principal differences between these constructions. *First*, what is being compared? Defendants' construction compares digital content identifiers with ***other*** digital content identifiers. IV compares something different: "files" (as opposed to digital content identifiers) with digital content identifiers. But IV's construction conflicts with the claim language on its face; the latter compares the "digital content identifiers" against "other digital identifiers." This analysis is further bolstered by the preceding step in claim 22, in which the digital content identifiers are outputted to the "server." JC Ex. A at 1 (agreed construction). Thus, the server that is performing the comparison in the disputed term has the digital content identifier. The server may not have the file itself, however. The logic of the claims dictates that the comparison use the identifier that the server has received, rather than a file to which it may not even have access.

Second, what does "characterizing" mean in the context of these claims? Claim 22's surrounding text supplies the answer. The step after the phrase in dispute requires "indicating the presence or absence of a characteristic." JC Ex. C, '050 Col. 10:5-6. This "characteristic" is simply the result of the "characterizing" of the disputed phrase. As demonstrated in § III(B)(1), supra, "indicating the presence or absence of a characteristic" requires "providing the result of a true/false test." This means that the classifying done in the disputed phrase must likewise be

based on the result of a true/false test.

C. The '142 Patent

The '142 patent purports to provide more efficient ways for corporate organizations to control the handling of e-mails and other data objects. JC Ex. E, '142 Col. 3:2-6. The '142 patent generally describes automatically deferring and reviewing e-mail messages and other data objects by applying business rules to the messages as they are processed by post offices of the organization before forwarding to intended recipients. *Id.* Abstract. "Each business rule describes a particular action to be applied to an e-mail message in response to either attributes of the e-mail message or performance data of the post office." *Id.* 3:30-33. "The attributes of an e-mail message which may trigger application of a business rule include, for example, the size of the e-mail message, the number of attachments, the size of individual or all attachments, the text of the message or its subject line, the inclusion of specific addresses or distribution lists, and other message-specific attributes." *Id.* 3: 39-45.

IV asserts 9 claims: independent claims 1, 17, 18, 21, 22, and 24-26, and dependent claim 7. The parties present seven claim construction disputes.

i. "Business rule[s]"

The parties dispute the meaning of "business rule," as follows:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"business rule[s]"	"a statement of an antecedent condition and the action to be applied when that antecedent condition is satisfied"	"plain and ordinary meaning"

IV's proposal that this disputed phrase need not be construed is legally inappropriate, *O2 Micro*, 521 F.3d at 1361. The disputed claim language viewed in context, *IGT*, 659 F.3d at 1116-17, and the specification point the same way. Because claim phrases are presumed to have the same scope even though they appear in different claims, *e.g.*, *Fin. Control Sys. Pty, Ltd. v. OAM, Inc.*, 265 F.3d 1311, 1318 (Fed Cir. 2001), we assess this disputed claim phrase in claim 1 as representative of all the independent claims.

In disputed claim 1, the disputed limitation requires "a database of business rules, each business rule specifying an action for controlling the delivery of an e-mail message as a function of an attribute of the e-mail message." JC Ex. E, '142 Col. 27:7-10. Hence a "business rule" in the claims must be able to (1) specify an action to control the delivery of an e-mail message, and (2) do so based on an attribute of that e-mail message. For example: "(1) do not deliver an e-mail message if (2) the e-mail message is larger than 10 megabytes." Simply as a matter of logic, the only way for that limitation to be satisfied is for a business rule to state an antecedent condition and the action to be applied when that antecedent condition is satisfied. (Otherwise, nothing controls the delivery of an e-mail message based on an attribute of the e-mail message; the e-mail message is simply delivered, irrespective of its attributes.) Indeed, this is the normal sense of a "rule." For example, if a pleading is filed that does not conform to this Court's Local rules, the Court, in its discretion, may give notice that it will not act on the matter raised until the defect is corrected. D. Del. LR 5.1.2. There is a statement of an antecedent condition ("if a document is filed that does not conform to the Rules") and the action to be applied when that antecedent condition is satisfied (the Court may decline to act).

The specification—"the single best guide to the meaning of a disputed term," *Phillips*, 415 F.3d at 1315—provides the same guidance. Figure 8 "illustrates a sample user interface … ***for defining business rule.***" JC Ex. E, '142 Col. 15:55-56. As Figure 8, reproduced to the left, shows, "[e]ach rule has an antecedent and a consequent." *Id.* 15:58. "Once the antecedent [the "IF" illustrated in Figure 8] is defined, the administrator defines the rule consequent [the "THEN" illustrated in Figure 8] by specifying the action to be applied to a message satisfying the antecedent conditions." *Id.* 16:4-7. Defendants' construction most naturally aligns with

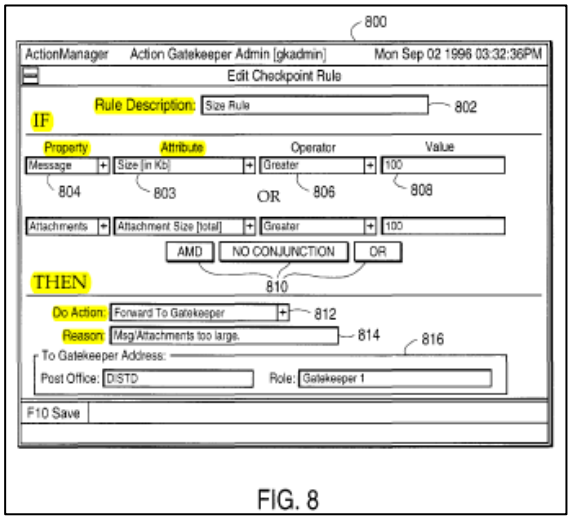


FIG. 8

the claim language and the specification, *Phillips*, 415 F.3d at 1315, and it would be appropriate to adopt it. So, too, of the next dispute: "database of business rules."

ii. A "database of business rules" is not limited to a "data structure"

The parties' dispute here crystallizes into whether a "database," as used in these claims, is limited to a "data structure," as IV urges.

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"database of business rules"	"storage of statements that each specify an antecedent condition and the action to be applied when that antecedent condition is satisfied"	"a data structure that stores one or more sets of business rules"

Nothing in the disputed claim language or its surrounding context limits a database to a "data structure"—whatever that undefined phrase means, *see Girafa.com, Inc. v. IAC Search & Media*, 653 F. Supp. 2d 512, 518 (D. Del. 2009) (Stark, J.) (declining to adopt a proposed construction substituted one confusing term for another). And the specification points away from IV's construction. It states merely that "[t]he rules ***may*** be internally stored . . . by any of a number of useful implementing data structures." JC Ex. E, '142 Col. 16:42-44. Not that they must; simply that they "may." In normal usage, "may" is permissive, not mandatory. Hence defendants' construction: storage of the business rules (with "business rules" defined as above).

iii. "An organizational hierarchy of a business" is not just "organizational information" about a business

Here, as elsewhere, IV's "construction" of this disputed claim phrase largely repeats the words and phrases to be construed, this time while reading out an express requirement of the claims: the organizational hierarchy. The parties' dispute is:

\

\

\

\

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"an organizational hierarchy of a business, the hierarchy including a plurality of roles, each role associated with a user"	"a business's rankings of its roles, containing multiple levels and each level comprising at least one organization role to which at least one individual is assigned"	"organizational information of a business, including a plurality of roles, each role associated with a user"

The parties' dispute largely centers around the phrase "organizational hierarchy." This limitation is directed to an organizational hierarchy of a business, suggesting that normal English usage, not some specialized or peculiar computer-specific usage, will guide construction of that term. The ordinary and customary meaning of "hierarchy" is "any system of persons or things ranked one above another." Winters Ex. 2, *The Random House Unabridged Dictionary* at 901 (2ND ed. 1993). IV, however, would read "hierarchy" and its core meaning out of the claims. That would violate abundant precedent that limitations are not superfluous. *E.g.*, *Merck & Co. v. Teva Pharms. USA, Inc.*, 395 F.3d 1364, 1372 (Fed. Cir. 2005).

In addition, the specification points away from IV's proposal. The specification contrasts "organizational hierarchy" with "organizational information":

> An organizational database 111 stores ***organizational information, <u>including</u> an organizational hierarchy*** of organizational roles and the individuals assigned to such roles. This information is used by the REPOs 102 and GPOs 106 to apply various rules to messages based on the role of the sender or recipient.

JC Ex. E, '142 Col. 6:8-13. The specification confirms that an "organizational hierarchy" can be part of "organizational information," but the latter is broader than the former. The "organizational hierarchy" in the claims refers to a type, but not all, of "organizational information;" the two are not coextensive. IV is not free now in litigation to disregard the claim language and the specification in an effort to enlarge claim scope. *Southwall Tech.*, 54 F.3d at 1578.

iv. "Combin[ing] the e-mail message . . . ."

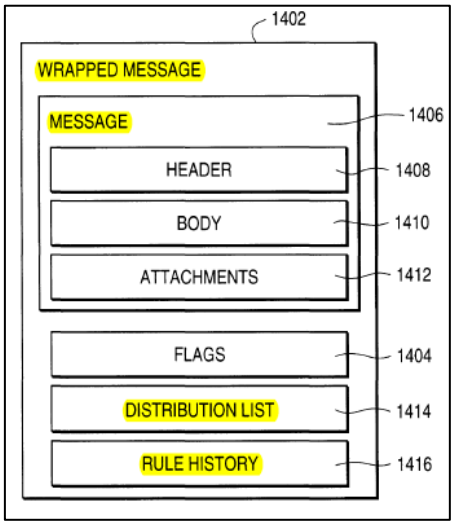
The full extent of the parties' disputed claim phrases appears in Appendix B hereto. Using claims 17 and 21 as representative, the dispute is:

\

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"combining the e-mail message with a new distribution list … and a rule history specifying at least one business rule determined to be applicable to the e-mail message" (claims 17, 21)	"combining the e-mail message [data object], a new distribution list, and a rule history into a wrapped message" "rule history": "a list identifying each of the [or at least one] business rule[s] whose antecedent condition was satisfied by the e-mail message [or data object]"	"Affixes/Affixing to the e-mail message (1) address information for at least one new destination post office for receiving the e-mail message for review by an administrator associated with the destination post office, (2) information identifying the reasons [or at least one reason] why the e-mail message was designated for administrator review by at least one rule engine"

At bottom, there are two disputes: (1) the meaning of "combines/combining" and (2) the meaning of "rule history." For the first, IV argues that "combines/combining" means simply "affixes/affixing." That proposal conflicts with the plain language of the claims. The claim language requires "combining" [1] the e-mail message with [2] a new distribution list and [3] a rule history specifying at least one business rule determined to be applicable to the e-mail message. The claim language does not require merely affixing (or attaching) a new distribution list and a rule history ***to*** the e-mail message or data object.

IV's proposal is also inconsistent with the specification. *Phillips*, 415 F.3d at 1315. Nowhere in the specification does it describe merely affixing a distribution list or a rule history to the e-mail message or data object. Rather, the specification describes a "wrapped message," which contains the e-mail message, distribution list, and rule history, as the figure reproduced on the left ('142 Fig. 14) shows. The specification explains that "the distribution engine 230 first ***wraps*** 1324 ***the message object*** and the action list into a wrapped message . . . . The wrapped message 1402 contains ***a distribution list*** 1414 of all the GPOs 106 that are to review the message based on the rules that fired . . . . The wrapped message 1402 also contains ***a rule history*** 1416 of the reasons why



the message was removed from the normal distribution stream." *Id.* 20:43-62. In other words, the specification describes combining e-mail message or data object, a distribution list, and a rule history into a single entity, *i.e.*, a wrapped message. Here as elsewhere, defendants' construction stays true to the claim language and most naturally aligns with the patent's description of the invention. *Phillips*, 415 F.3d at 1316.

In the "rule history" dispute, IV improperly broadens the claims by proposing that "rule history" means "information identifying the reasons [or at least one reason] why the e-mail message was designated for administrator review . . . ." The plain language of the claims, however, requires that "a rule history ***specif[ies]*** [the or at least one] business rule[s] [that were] determined to be applicable to [e-mail message or data object]." JC Ex. E, '142 Cols. 27:27-28, 29:55-56, 31:3-5, 31:26-28, 32:30-33 & 34:1-3. As discussed above, a "business rule" is "a statement of an antecedent condition and the action to be applied when that antecedent condition is satisfied." A rule history does not merely identify the reasons why the e-mail message or data object was designated for administrator review, but lists ***specific rules*** that were actually determined to be applicable to the e-mail message or data object. Accordingly, defendants' construction of "rule history" as "a list identifying each of the [or at least one] business rule[s] whose antecedent condition was satisfied by the e-mail message [or data object]" is correct.

v. The "persistently storing" claims

Using claim 7 as representative, the parties present three disputes for construction:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"persistently storing" (claims 7, 21, 22, 25, 26)	"storing for extended periods of time"	"storing in memory that remains intact when a device is turned off, but not necessarily permanent storage"
"primary message store… for receiving and non-persistently storing e-mail messages" (claim 7)	"a first mechanism that stores short lived email to which the rules do not apply"	"plain and ordinary meaning"
"secondary message store…for receiving therefrom, and persistently storing an e-mail message" (claim 7)	"a second mechanism that stores emails to which at least one rule applies"	"plain and ordinary meaning (apart from "persistently storing," defined above)"

IV's construction is not consistent with the language in this disputed limitation. The limitation requires persistently storing so that an administrator can review the e-mail message at some indeterminate future point: "persistently storing an e-mail message in response to the rule engine specifying the action that the e-mail message be reviewed by an administrator recipient prior to delivery to a specified recipient." JC Ex. E, '142 Col. 28:27-31. That administrator review could happen quickly, or only after a delay. The claim encompasses both possibilities, and in the latter, the e-mail message would need to be stored for an extended period of time. Hence defendants' construction: "storing for extended periods of time." Contrary to IV's proposal, the claim language does not require, and indeed says nothing about, maintaining the "memory intact" (whatever that means) while the secondary message store is turned off.

The specification confirms, however, confirms defendants' construction. It states that "[t]he message store 250 generally provides for temporary storage of message objects for subsequent distribution by the distribution engine 230. . . . to enable the rule engine 210 to access stored messages for processing prior to any distribution." *Id.* 6:43-50. Nothing in that language requires maintaining the memory intact while the message store is turned off. Instead, the specification discloses merely that the message may need to be stored for an extended period of time to allow for administrator review. *See also id.* 8:37-38 ("may require storage for extended periods of time") & 9:34-41 ("gated messages which tend to have relatively long or persistent storage").

Here as elsewhere, IV's proposal that that the Court need not construe a disputed limitation—"primary message store . . . for receiving and non-persistently storing e-mail messages"— runs afoul of *02 Micro*, 521 F.3d at 1361. And the disputed language in the context of the entire claim confirms defendants' construction: "a first mechanism that stores short lived email to which the rules do not apply."

Claim 7 is directed to "[t]he post office of claim 1, further comprising," first, "a primary message store, coupled to the receipt engine, for receiving and non-persistently storing e-mail messages." That language informs that the "primary message store" is a thing as opposed to a

process, because it is part of "[t]he post office of claim 1" and is also "coupled to the distribution engine." (Indeed the specification's Background of the Invention specifically states that "post offices are distribution mechanisms[.]" JC Ex. E, '142 Col. 1:38-44.) The "primary message store" also serves a function: to receive and non-persistently store e-mail messages. The limitation says nothing about applying rules to these non-persistently stored e-mail messages.

Claim 7's second limitation, however, requires applying the rules to the e-mail messages discussed in that limitation. But those e-mail messages are "persistently stor[ed]" in a "secondary message store," *i.e.*, a message store different from the first, and are "persistently stor[ed] . . . in response to the rule engine specifying the action that the e-mail message be reviewed by an administrator recipient prior to delivery to a specified recipient." In plainer English, the rules apply to the persistently stored e-mails, but not to the non-persistently stored e-mails. The claim language points towards this construction.

So do the prosecution history and the specification. During prosecution, the patent office explicitly states that this disputed first limitation would have been obvious in light of specified art "because this would help in the management of short lived mail to which the rules do not apply." JC Ex. O, '142 FH, 06/08/99 Office Action at 4. The patent office specifically contrasted this second limitation with the third, stating that the third limitation would have been obvious "because this would help in the management of mail to which at least one rule [did] apply." *Id*. at 5. Although the applicants successfully avoided this prior art, they did not thereafter dispute that understanding of this limitation. Moreover, the specification specifically distinguishes short-lived e-mail from e-mail to which at least one rule applies. JC Ex. E, '142 Cols. 8-45-47 & 9:34-41.

Finally, the language surrounding the final disputed phrase in claim 7 ("secondary message store . . . for receiving therefrom, and persistently storing an e-mail message") supports a construction as "a second mechanism that stores emails to which at least one rule applies," as defendants submit. The claim language on its face differentiates between the "primary message store" of the first limitation and the "secondary message store" of the second limitation.

Likewise, and as explained above, the claim language of the second limitation requires that at least one rule apply to the persistently stored e-mails of that second limitation; but the first limitation contains no such requirement. And the same prosecution history and specification sections that guided construction of the first limitation also guide construction of the second.

vi. "Rule engine" must be construed

As elsewhere, IV seeks to avoid construction of a disputed term in a claim that it elected; *02 Micro* again bars that effort. The claim language and the specification again align to point towards defendants' construction.

Claim 7, for example, is directed to "[t]he post office of claim 1." The Background of the Invention states that "post offices are distribution mechanisms," JC Ex. E, '142 Col. 1:39-40, and the Summary of the Invention states that "a post office includes . . . a rule engine," *id*. 3:22-24. Hence a "rule engine" is a mechanism. And it applies business rules. The claim language makes this clear on its face in specifying "persistently storing an e-mail message in response to the rule engine specifying the action that the e-mail message be reviewed by an administrator recipient prior to delivery to a specified recipient." *Id*. 28:27-31. In plainer English, the rule engine applies the business rules, in order to determine a set of actions to be applied.

The specification corroborates the point. The Summary of the Invention, which as explained above receives great weight in claim construction, explains that "[i]n accordance with the present invention, the rule engine operates with the database to apply the business rules to each e-mail message, in order to determine a set of actions (one or more) to be applied to the e-mail message," *id*. 4:8-12, and that "[t]he rule engine provides for each e-mail message it processes a set of actions to the distribution engine. The distribution engine is responsible for handling the e-mail message according to the set of actions," *id*. 4:21-24. Even beyond these clear and weighty pointers, the Summary of the Invention repeats the disclosure that a rule engine applies the business rules, in order to determine a set of actions to be applied. *Id*. 4:31-33

("The distribution engine then reviews the set of actions and applies the action having the highest priority level."). The detailed description makes the same point, repeatedly.[3]

The claim construction path here is clear: "Rule engine" means "a mechanism that applies the business rules, in order to determine a set of actions to be applied"; contrary to IV's litigation position, this term has no "plain and ordinary meaning."

vii. The "automatically reviewing" limitations

As *Phillips* underscored, "the context in which a term is used in the asserted claim can be highly instructive," 415 F.3d at 1314, and "[u]ltimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim," *id*. at 1316. Here, the disputed limitations of these two independent claims are best understood by considering the context of the claim language that surrounds them, because by the time the "e-mail message" or "data object" of claims 22 and 25 are the subject of their respective disputed limitations, much has happened to them. Under IV's construction, however, these previous steps in the method are essentially without meaning.

Claim 22 defines a seven-step "computer implemented process for reviewing an e-mail message." JC Ex. E, '142 Col. 31:16-38. In the steps before the disputed sixth limitation, delivery of the e-mail message as originally received has been deferred, and it has been directed to a second post office. The e-mail message has been combined with a new distribution list and a rule history specifying at least one business rule that applies to the message. It will be

[3] *E.g.*, JC Ex. E, '142 Cols. 6:58-60 ("The rule engine 210 operates in conjunction with a rule base 270 to process incoming messages with business rules defined in the rule base 270."); 6:66-7:3 ("Each business rule specifies an action to be applied to a message by the distribution engine 230. The actions are output by the rule engine 210 in the form of an action list which is read and interpreted by the distribution engine 230."); 11:63-12:7 ("If the message has expired, the GPO 106 invokes the rule engine 283, which processes the message against the rules in the gatekeeping rule base 289 to determine an appropriate action."); 17:36-39 ("For each message, the rule engine 210 generates an action list of one or more actions to be performed by the distribution engine 230 on the message.").

persistently stored at that second post office until it is reviewed.

IV's construction simply ignores this context and in particular the prior steps of the method. Under IV's construction, the prior steps in the method are essentially without meaning. The parties disagree as follows:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"automatically reviewing the email message after a specified time interval to determine an action to be applied" (claim 22)	"after a specified period of time, applying at least one business rule of 'the second post office' to the selected e-mail message to determine an action to be applied"	"computer determination of an action to be applied to the email message after a specified period of time"

IV's construction of this disputed limitation is not consistent with the language of the claim as a whole, as it must be. *IGT*, 659 F.3d at 1116-17. Under IV's construction, the previous steps in the method are essentially deleted. The e-mail message arrives at the second post-office and, even though delivery was delayed and the e-mail message was combined with other information, the second post office's rules may not have anything to do with how the e-mail is processed by the second post office. The structure and logic of the claim as a whole rejects the notion that the "action to be applied" in the sixth step of the method be completely untethered from the previous steps in the method—that is, the context and state in which the e-mail message arrives at the second post office.

So does the specification. The Abstract, for example, states that "the message is automatically reviewed by the gatekeeping post office [*i.e.*, the second post office] ***with its own set of business rules***." JC Ex. E, '142 Abstract. In fact, the Abstract extols the benefits of having a second post office apply its own set of rules: "[h]aving multiple post offices with independent sets of business rules allows for distributed and hierarchical review and gating of the messages." The Summary of the Invention likewise extols the benefits of having a second, gatekeeping post office apply its own set of rules to the e-mail messages that it has received for processing: "The gated e-mail messages may also be automatically processed by an independent set of business rules, and again various different actions may be applied. Because ***each***

gatekeeping post office may act independently, it may further gate the e-mail message to yet another gatekeeping post office. This enables distributed, network gatekeeping and review of the e-mail messages by any number of corporate officials designated as gatekeepers." *Id.* 4:47-54.

Hence, in the context of the claim and the specification, the most sensible and natural reading of the disputed phrase ("automatically reviewing the e-mail message after a specified time interval to determine an action to be applied to the e-mail message") is to mean that after some specified period of time at the second post office, at least one business rule of that second post office is applied to the e-mail message to determine an action to be applied. If the second post office were to apply a rule from the first post office, the second post office would serve essentially no function. It would act as a pass-through. As elsewhere, the claim language and the specification align to support defendants' construction and reject IV's.

The final disputed '142 limitation is claim 25:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"automatically reviewing the data object after a specified time interval to determine an action to be applied" (claim 25)	"after a specified period of time, applying at least one business rule defined by 'the recipient other than a specified recipient' to the data object to determine an action to be applied"	"computer determination of an action to be applied to the data object after a specified period of time"

In this claim as a whole, the business' organization hierarchy is stored in a database, and based on a database of business rules, deferring the delivery of a "data object" based on the user's role in the hierarchy (*e.g.*, "delay e-mail of more than 10 megabytes to the CFO"). Instead, the deferred "data object" is delivered "to a recipient other than a specified recipient." The data object is persistently stored until it is reviewed. Then comes the next step in the seven-step process: "automatically reviewing the data object after a specified time interval to determine an action to be applied to the data object."

In the context of that claim as a whole, the construction that most naturally aligns with the claim language is defendants': after a specified period of time, applying at least one business rule defined by 'the recipient other than a specified recipient' to the data object to determine an

action to be applied. In plainer English, that a rule defined by the transferee-recipient of the data object be applied to determine what to do with the data object. Otherwise, as in claim 22, the redirection of the data object to a user other than a specified recipient is essentially pointless; the transferee-recipient acts essentially as a pass-through.

The discussion above, about the Abstract and the specification's discussion of e-mail messages, apply equally claim 25's discussion of "data objects," because as the Abstract states, "[t]he system can route any type of data object, and apply the business rules to such objects in a similar manner." Here, again, the claim language and the specification align to support defendants' construction and reject IV's.

D. The '610 Patent

The '610 patent is directed to "screen[ing] computer data for viruses within a telephone network before communicating the computer data to an end user." JC Ex. D, '610 Col. 1:59-61.[4] The '610 patent distinguishes prior art in which viruses were screened on users' computers. *See id.* at 2:20-23 ("Consequently, each computer user has to repeatedly upgrade the virus screening software installed on his/her computer to ensure protection from recently-discovered viruses.").

IV asserts claim 7, a method claim depending from claim 1. The parties present three disputed phrases from these claims.

i. "Routing a call . . . ."

The key phrases in this first disputed term are "routing a call" and "telephone network." IV's construction conflicts with the plain meaning of both "routing" and "call," and reads "telephone network" out of the claims. The parties' dispute is:

\

\

\

[4] The '610 patent issued to to Ameritech Corporation, a regional Bell telephone company. Winters Ex. 4, *Newton's Telecom Dictionary*, 37 (11th ed. 1996) (defining "Ameritech").

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"routing a call between a calling party and a called party of a telephone network"	"determining and securing, for a call, the communication path between the telephone line of a calling party and the telephone line of a called party"	"transmitting a voice or data transmission between a party initiating a voice or data transmission and a party receiving a voice or data transmission"

"Routing a call" means "determining and securing, for a call, the communication path." This construction is supported by the plain meaning of the claim language itself, as well as the specification. The surrounding claim language refers to a "calling party," a "called party," and "communication" from one party to the other, and makes clear that the structural context in which the recited steps of the claimed method are executed is a "telephone network" through which a path must be established. Further, the specification explicitly describes how a "route" through the telephone network is "determined" by "securing an appropriate path." JC Ex. D, '610 Col. 3:39-41 ("[T]he telephone network 10 determines and secures an appropriate path for the duration of the call."); *id.* 3:41-43 ("[T]he path can be determined to include a route through a processor which examines the contents of information being passed during the call.").

This construction of "routing a call" also gives that phrase "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips*, 415 F.3d at 1313. For example, a contemporaneous edition of the *IEEE Standard Dictionary of Electrical and Electronics Terms*, 937 (6th. ed. 1996) defines "routing" as:

> (A) In data communications, a path by which a message reaches its destination (B) A path that network traffic takes from its source to its destination.

Winters Ex. 3. Other dictionaries, both telecommunications-specific and general, are consistent. Winters Ex. 4, *Newton's Telecom Dictionary*, 520 (11th ed. 1996) (defining "routing" as "[t]he process of selecting the correct circuit path for a message."); Winters Ex. 5, *McGraw-Hill Dictionary of Scientific and Technical Terms*, 1734 (5th ed. 1994) (defining "routing" as "[t]he assignment of a path by which a message will travel to its destination."). These reflections of the ordinary artisan's understanding recognize that "routing" requires "a path" between source and destination.

IV's proposal that "routing" simply means "transmitting" ignores the ordinary meaning of the word "routing," which requires the determination of a particular route or path. Indeed, one may "transmit" something that never reaches its destination, or reaches its destination over routes determined by external factors, or by broadcasting to many destinations without regard for the route taken. Here, the claims require "routing," not mere "transmitting," and the only type of "routing" consistent with the specification is determining a path for a call through the telephone network.

Additionally, the specification draws a clear distinction between "routing" and "transmitting," using these words in disparate contexts, with "routing" connoting the assignment of a path or direction, while "transmitting" merely connotes sending, without regard for the route taken. *Compare* JC Ex. D, '610 Col. 5:40-50 ("[T]he SCP 92 can *direct the call to be routed though a network node* appropriately equipped for virus screening"), *with id.* 4:58-60 ("[E]ach of the virus-screening processors can have one or more associated modems *to modulate computer data for transmission* [*i.e.* prepare it for sending]").

IV proposes that "call" means "voice or data transmission," but this proposal is inconsistent with the plain meaning of the word "call," which virtually anyone can understand in the context of a telephone network (*i.e.* a telephone call). *Phillips*, 415 F.3d at 1314 ("In some cases, the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words."). Moreover, the specification clearly discloses that a "call" must be routed prior to the transmission of data. For example, in the flow chart in Figure 3, data may be received and communicated (at steps 106 and 110) only after a call has been routed (at step 104), and before the call is terminated (at step 124). IV's proposal, which directly equates a "call" with a "voice or data transmission," is inconsistent with this teaching and is thus wrong.

"Between a calling party and a called party of a telephone network" means "between the telephone line of a calling party and the telephone line of a called party." The claims point

towards this construction. There, it is clear that the recited steps occur in the context of a "telephone network." Indeed, the phrase "telephone network" appears four times in independent claim 1. And, as discussed above, the word "call," as used in "calling party" and "called party," has a well-known plain meaning in the context of a telephone network—a telephone call. A "call" may carry voice traffic, as in the case of the typical telephone conversation between two people, or data, as in the case of two computers communicating over a dial-up modem connection. But either way, the claims require a "call" placed across a telephone network.

The summary portion of the specification confirms that the system operating "in accordance with ***the present invention*** … includes a ***telephone network*** 10 to serve a plurality of ***telephone lines*** 12." JC Ex. D, '610 Col. 2:2-4.[5] "[R]egardless of its form," whether public or private, the telephone network of the alleged invention "communicate(s) signals ***between telephone lines***." *Id.*, 2:4-15; *see also id.* 2:33-36, 2:46-49. These descriptions of "the present invention" are definitional. *Verizon Servs.*, 503 F.3d at 1308. Telephone lines are integral to the alleged invention, are disclosed in every embodiment described, and therefore any construction of "telephone network" requires "telephone lines." *See Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1367-68 (Fed. Cir. 2007) (limiting claim term in light of statements in specification that are "not descriptions of particular embodiments, but are characterizations directed to the invention as a whole").

IV's proposal is wrong because it reads the language "of a telephone network" completely out of the claim, violating the rule that every word in a claim must have some meaning. *See, e.g., Digital-Vending Servs. Int'l, LLC v. Univ. of Phoenix, Inc.*, 672 F.3d 1270,

[5] The Code of Federal Regulations required applicants to include a summary under the heading "Brief Summary of the Invention." 37 C.F.R. § 1.77 (1998). The '610 patent applicants omitted the heading and instead provided a Summary of the Invention within the "Detailed Description" between 1:57 and 5:10, after which they discussed the preferred embodiments. *See, e.g.*, JC Ex. D, '610 3:1-13 (teaching general aspects of method and concluding, "A preferred embodiment of a virus screening method is subsequently described in detail with reference to Fig. 3."), 1:25-55 (indicating Figs. 1 and 2 depict the telephone network and other figures, which are described staring at 5:11, depict embodiments of claimed method and system).

1275 (Fed. Cir. 2012) (citing *Phillips*, 415 F.3d at 1314). Omitting words from the claim also threatens to undermine the notice function that claims provide. *Phillips*, 415 F. 3d at 1312 ("Because the patentee is required to define precisely what his invention is ... it is unjust to the public, as well as an evasion of the law, to construe it in a manner different from the plain import of its terms.") (quoting *White v. Dunbar*, 119 U.S. 47, 52 (1886)). IV's proposal that "telephone network" be read out of the claim would result in an outcome that would be unjust in light of these considerations.

ii. "Within the telephone network"

The parties' dispute is:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"within the telephone network"	"in and between nodes that communicate signals between pairs of telephone lines"	"in the voice or data network connecting the calling party and called party, exclusive of the networks of the called party and calling party"

Defendants' construction of this term reflects the ordinary understanding of the term, the teachings of the specification, and the disavowals of scope made during the prosecution history. The words "telephone network" are the kind of claim language the Federal Circuit had in mind when it held that "[i]n some cases, the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges." *See Phillips*, 415 F.3d at 1314. In a patent assigned to Ameritech that describes virus screening during calls at computers connecting pairs of telephone lines, the ordinary meaning of "telephone network" is clear.

The specification and prosecution history are consistent with the plain meaning. The summary section of the specification teaches that "the computer data can be screened [for viruses] at any *node* in the telephone network." JC Ex. D, '610 2:58-59 (emphasis added); *see also id.* 3:34-38. As explained above, the nodes of a "telephone network" exist between the telephone lines of the calling and called parties. *See also id.* claim 12, 15:28-40 (reciting "a telephone switching node to route a call between a calling party and a called party")

During prosecution, the patentees added to claim 1 the limitation "within a telephone network" to overcome a § 102(b) rejection over Hile, which teaches that virus screening is performed on the destination computer. JC Ex. K, '610 FH, 06/28/99 Response at 4-5. The patentees explained that "[a]mended claim 1 clearly distinguishes over Hile by detecting, *within the telephone network*, a virus in the computer data…." *Id.* at 5 (emphasis in original). With this statement IV surrendered instances where virus screening occurs at the destination computer (which is not "within" the telephone network, but rather is an endpoint of the network), and where screening does not occur in and between the nodes of the network that communicate signals between telephone lines. *Phillips*, 415 F.3d at 1317 ("[T]he prosecution history can often inform . . . whether the inventor limited the invention during the course of prosecution . . . .").

IV's proposal that "telephone network" means "voice or data network" is inconsistent with the language of the claim and the specification. First, IV's proposal improperly reads the word "telephone" out of the claim, and for the reasons discussed above, this is improper. Second, IV's proposal leads to ambiguity and confusion because it offers no separate definition of what a "voice or data network" would be. Although the telephone network described in the specification may be used to carry voice and data communications within a call, those communications are always described as being carried over a "telephone network," and never over a "voice network," a "data network," or a "voice or data network." Accordingly, IV's proposal is unsupported, is confusing, and is simply wrong.

iii. "Identification code" means "a set of symbols that identify"

The parties' dispute is:

Disputed Claim Phrase	Defendants' Construction	IV's Construction
"identification code"	"a set of symbols that identify"	"telecommunications or other network address"

Defendants' construction of "identification code" is consistent with the intrinsic evidence and plain meaning of the term. The term "identification code" only appears once in the description of the alleged invention. In a discussion of the "routing" step 102 shown in Figure 3,

the specification explains that "a query to a database ... can include an identification code of the calling party and/or an identification code of the called party." JC Ex. D, '610 Col. 5:21-26. Defendants' definition of "identification code" is fully consistent with this appearance.

Defendants' construction is also consistent with the ordinary understanding of the word "code," as evidenced by contemporaneous dictionaries. *See, e.g.*, Winters Ex. 5, *McGraw-Hill Dictionary of Scientific and Technical Terms*, 397 (5th ed. 1994) (defining "code" as "[a] system of symbols and rules for expressing information . . . .").

In contrast, IV's proposed construction, "telecommunications or other network address," is inconsistent with the specification, the prosecution history, and the plain meaning of "code." First, an "address" is not the same thing as a "code," either by plain meaning or as used in the specification. The specification uses both the word "address" and the word "code," but never associates the two together. IV is not simply trying to read the claim language in light of the specification, which is appropriate and indeed required. Instead, IV is trying nakedly to import a limitation into the claims. Absent a clear disclaimer of claim scope in the specification, which IV could not argue here, that is improper. *Andersen*, 474 F.3d at 1373.

Even if "address" and "code" were synonymous in the patent (and they are not), a "telecommunications address" as IV proposes still would not have the same meaning as "identification code." During prosecution, the Examiner and applicants agreed that as recited in claim 8 a "telecommunication code" meant something different from "identification code." For example, in an Office Action, the Examiner read "identification code" onto a "virus ID" disclosed in Hile. JC Ex. K, '610 FH, 03/23/99 Office Action at 3. In response, the applicants distinguished claim 7 over Hile on other grounds, but did not contest that a "virus ID" was an "identification code." *Id.*, 06/28/99 Response at 5-6. That is, the applicants and the Examiner both agreed that an "identification code" was broader than a "telecommunication code."

IV appears to acknowledge that "identification code" must be broader than "telecommunications address" and therefore has proposed to add "or other network address" in its construction. But this language is vague and will be unhelpful to the jury. In IV's proposed

construction, it is unclear what types of addresses, let alone codes, would fall within the scope of the claim. For these reasons, IV's proposal is incorrect and unsupported.

IV. CONCLUSION

The claim language, specification, and prosecution histories of these patents light a clear and well-lit path to correct claim construction in this dispute. Defendants respectfully ask that the Court adopt defendant's proposed constructions explained herein.

Dated: June 5, 2012

SEITZ ROSS ARONSTAM & MORITZ LLP

/s/ Benjamin J. Schladweiler
Collins J. Seitz, Jr. (Bar No. 2237)
Benjamin J. Schladweiler (Bar No. 4601)
100 S. West Street, Suite 400
Wilmington, DE 19801
(302) 576-1600
cseitz@seitzross.com
bschladweiler@seitzross.com

Attorneys for Defendant McAfee Inc.

OF COUNSEL:

Edward G. Poplawski, Esquire
Sandra S. Fujiyama, Esquire
Olivia M. Kim, Esquire
SIDLEY AUSTIN LLP
555 West Fifth Street, Suite 4000
Los Angeles, CA 90013
Telephone: (213) 896-6000

Vernon M. Winters, Esquire
SIDLEY AUSTIN LLP
555 California Street, Suite 2000
San Francisco, CA 94104
Telephone: (415) 772-1200

Bryan K. Anderson, Esquire
SIDLEY AUSTIN LLP
1001 Page Mill Road
Palo Alto, CA 94304
Telephone: (650) 565-7000

OF COUNSEL:

Yar R. Chaikovsky, Esquire
MCDERMOTT, WILL & EMERY LLP
275 Middlefield Road, Suite 100
Menlo Park, CA 94025

David M. Beckwith, Esquire
MCDERMOTT, WILL & EMERY LLP
4 Park Plaza, Suite 1700
Irvine, CA 92614-2559

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Karen Jacobs Louden
Karen Jacobs Louden (Bar No. 2881)
Michael J. Flynn (Bar No. 5333)
1201 North Market Street
Wilmington, DE 19899
(302) 658-9200
klouden@mnat.com
mflynn@mnat.com

Attorneys for Defendants Trend Micro Incorporated and Trend Micro, Inc. (USA)

OF COUNSEL:

Clement S. Roberts, Esquire
Joseph C. Gratz, Esquire
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111

Attorneys for Defendants Check Point Software Technologies Inc. and Check Point Software Technologies Ltd.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jack B. Blumenfeld
Jack B. Blumenfeld (Bar No. 1014)
Thomas C. Grimm (Bar No. 1098)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
tgrimm@mnat.com

Attorneys for Defendants Check Point Software Technologies Inc. and Check Point Software Technologies Ltd. and Symantec Corporation

OF COUNSEL:

Mark A. Flagel, Esquire
Yury Kapgan, Esquire
LATHAM & WATKINS LLP
355 South Grand Avenue
Los Angeles, CA 90071-1560

Dean G. Dunlavey, Esquire
LATHAM & WATKINS LLP
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626-1925

Andrew J. Fossum, Esquire
LATHAM & WATKINS LLP
717 Texas Avenue, 16th Floor
Houston, TX 77002
Telephone: (713) 546-7449

Attorneys for Defendant Symantec Corporation

Appendix A

How computer networks work

A network is an arrangement of computers and other components that allows computers to share information. A network can consist of personal computers, servers, and other hardware, like load-balancers, firewalls, and routers. Personal computers are computers that the user interacts with directly. In a network, they are often called clients because they receive information from one or more servers. Servers are more powerful computers which provide services (like providing files or web pages) to one or more clients. A network may also include other types of hardware. For example, it may include a load balancer, which distributes work among various servers, or a router, which routes incoming and outgoing messages to their intended recipients. Finally, most networks also include a firewall, or other security device, responsible for blocking harmful traffic from outside the network. These devices together act as a gateway to other networks.

Many networks are private, meaning they are under the control of a single entity, such as a corporation or government agency. Private networks can also be connected to a public network, for example, the Internet. The Internet is a public network because it consists of a set of publicly addressable computers that provide networking functions between and among the private networks that are connected to it.

Networks can be packet-switched or circuit-switched. Packet switching is a technique that breaks a message or data object into small pieces, or packets, each of which contains the address of its destination. The routers in the network independently route the packets towards their destination. Because the routing decisions are independent, packets from the same transmission may ultimately take different paths through the network. At the destination, the packets are reassembled into the original message or data object. Thus, in a packet switched network, the packets are dispersed into the network and do not follow a single path. Circuit switched networks, on the other hand, such as the public telephone network, use a different

transmission mechanism. In these networks, routers establish a single secured and dedicated channel (or "circuit") linking the endpoints for the duration of a particular transmission. All of the data for a given data object or message is sent over that channel. This is the way calls are handled by a normal telephone.

Networks, whether circuit-switched or packet-switched, can be either public or private. For example, the Internet is a public packet-switched network, and the public telephone network (also called the public switched telephone network, or "PSTN") is a public circuit-switched network. Similarly, private circuit switched networks are often found, for example, in office buildings that have a common phone number and extensions for individual offices. In many such buildings, there is a piece of hardware that takes an incoming call from the public circuit switched network and secures a dedicated transmission channel to the endpoint representing the dialed extension.

The point of connection between two networks is often called a gateway. Gateways can exist at the intersection of a public network and a private network, or at the intersection of a circuit-switched network and a packet-switched network. Thus, for example, it is common to refer to the set of routers, load balancers, and firewalls that provide network services for a particular private network as a "gateway" because that set of hardware works in tandem to provide an interface between the clients on the private network and the public network. Similarly, the phone company maintains a gateway between its circuit-switched network and the Internet. You can connect to a computer on the Internet through a dial-up or DSL line, both of which transmit signals over a telephone line. When dial-up or DSL is used, a modem is needed to generate signals for communication over the telephone line.

How e-mail works

Email is a particular type of data object. Each email contains a number of segments, including a header, a body, and, possibly, attachments. The header of an email is a portion of the email data file that contains information about where the email came from, to whom it is addressed, the time at which it was sent, the relay stations through which the email passed to

reach the destination, and other related information. The body of an email contains what we commonly think of as the text or content of the message, as well as information about the formatting and functionality of that content.

Thus, for example, the body of an email may contain a web page address along with formatting information to determine the appearance of the web address (for example, blue & underlined) and information about the function or process that may be called or invoked by activating that address.

Attachments are the third major component of an email data file, and they contain data that is generally intended to be accessed through an application separate from the one used to view the email. Thus, for example, an individual might receive and view an email in a program such as Microsoft Outlook, which has an attachment meant to be viewed in Microsoft Word. Attachments provide the ability to transmit additional content for use in another process or application.

The patents at issue in this case relate to technologies for dealing with incoming email. There are generally two types of unwanted email: 1) malicious email that contains viruses or other code intended to compromise the security of the computer or network; 2) unwanted but non-harmful email, such as unsolicited advertising (often called "spam").

How executable code including viruses work

A virus is a type of executable code, but it is, from the user's perspective, unauthorized. Viruses compromise the security of a computer or network. Viruses can be programmed to perform a wide variety of functions, including reporting keystrokes, changing network security settings, and transferring data. In order to perform these functions, however, viruses must be in a format that the computer recognizes as executable. That is, the virus must be in a format in which it is capable of causing the computer to take an action or to run some other process, such as a data transfer. Some viruses, for example, take the form of an executable attachment to an email. When the user double-clicks on the attachment to activate it, the email program asks the

computer to run the code constituting the attachment. When that code is run, it causes the virus to be stored in the computer's memory and to carry out the other tasks coded into the virus.

Another kind of virus is known as a macro virus. Macros are small pieces of code that are often invisibly embedded in word processing documents and used to format the document. A malicious author can write a macro virus, or a macro that acts like a virus by opening a process to carry out actions harmful to the computer. Macro viruses can be sent over email when a document containing a virus-laden macro is attached to the email. Other times, the malicious code may be in the form of a hypertext link. When the user clicks on such a link, it opens a browser application and may try to load a dangerous website.

The computer industry, since the earliest days of networks and viruses, has come up with many ways of finding and removing these malicious bits of code. This task can be complicated however, because viruses can take many forms, and because new ones are constantly being written. Traditionally, virus detection and elimination has been done at gateways that protect a network's edges. Those who own or operate private networks often invest in this technology to protect their networks from viruses entering the network from outside. For example, a provider may install a gateway firewall containing anti-virus software, which analyzes the messages passing through the gateway into the private network for viruses or other malicious code. Likewise, a provider may establish rules on its mail server to handle virus-laden emails differently than non-infected emails.

There are many ways to deal with a virus once it has been detected. Some anti-virus protection software deletes or quarantines the entire file that is infected with malicious code. For example, if the virus is contained in an e-mail, the e-mail may be deleted before it reaches the intended recipient. Alternatively, the e-mail may be quarantined; that is, diverted to a special mailbox where further human analysis may be performed on the e-mail to determine whether it is actually infected. If the virus is contained in an attachment to an e-mail, the attachment may be deleted before the e-mail reaches its intended recipient.

How spam and hashing work

The patents in suit are also concerned with the second kind of unwanted email – spam. Spam is not harmful per se; but it's like junk mail: it is often of no interest, and if the quantity is large enough, it can degrade network performance. Spam has existed since the early days of computer networks, and so have ideas for blocking it. The earliest anti-spam techniques were developed decades ago. They were able to determine if a given email was spam by using a database to tally how many times the network had seen the same email. It did this by storing the entire message, or a portion of the message, in a database. Spam, by its nature, is sent in bulk. Thus, if identical content was received many times over, it would be marked spam. Once certain email content was identified as spam, a program could effectively filter out any emails with that content.

However, the need to store each and every email or portion (and the associated count) received by anyone using a given system is expensive. Tracking so many emails requires a large database to store lots of data, and sending each email received to an anti-spam system requires lots of network bandwidth. These drawbacks led to the use of identifiers for tracking and counting emails. Rather than retransmitting and storing a lengthy spam email, a system might assign it an identifier which is sent and tracked instead. Once a particular identifier has been received a number of times, the system may determine that it represents spam. Every time an identifier is received, the system compares the new identifier to the ones it knows are spam; if it matches the email is considered spam and otherwise it is not.

One way of generating these identifiers is a technique called "hashing." A hashing function is a mathematical algorithm or formula that takes in some content and generates a tag that represents or identifies that content. For example, a lengthy Microsoft Word document might be hashed into a string of 64 alphanumeric characters. Depending on the hashing function used, these characters provide either a unique representation of the original document, or a representation that is shared by only a very small set of documents.

How e-mail rules work

Another approach for handling unwanted email is to create a series of rules that will be applied to an incoming email message. In this context, a rule is a simple if-then statement. The "if" portion is the antecedent condition that must be satisfied for the rule to apply; the "then" portion is an action that is applied to the email when the antecedent condition is satisfied. Rule-based mail systems subject each incoming email to the rules, determining, for each rule, if the antecedent condition is satisfied and then applying the action if it is.

For companies and organizations, these email rules run on their mail server (rather than the user's email program) so they can operate on all emails, rather than emails for a particular user. For example, one could have an email rule specifying that any e-mail destined to the CEO of a company should be accepted.

In many cases, an administrator will want to evaluate the email stopped by one or more rules to determine where (or if) it should be delivered. To facilitate that review, it may be helpful for the reviewer to have not only actions applied to the email, but also a history of the antecedent conditions that were satisfied – namely the rule(s) triggered by the email. These may be wrapped into or included in the message before being sent to the reviewer. Including such a history of the rules in the message allows for easier distribution to the reviewer and more efficient evaluation of the email by the reviewer. Alternatively, the message may be stored in a database with a record indicating what antecedent conditions were satisfied.

Appendix B

Disputed Claim Phrases	**Defendants' Construction**	**IV's Construction**
"combines the e-mail message with a new distribution list … and a rule history specifying the business rules that were determined to be applicable to e-mail message by at least one rule engine" (claim 1) "combining the e-mail message with a new distribution list … and a rule history specifying at least one business rule determined to be applicable to the e-mail message" (claims 17, 21) "combining the selected e-mail message with a new distribution list … and a rule history specifying at least one business rule determined to be applicable to the e-mail message" (claim 22) "combines the data object with a new distribution list … and a rule history specifying at least one business rule determined to be applicable to the data object by at least one rule engine" (claim 24) "combining the selected data object with a new distribution list … and a rule history specifying at least one business rule determined to be applicable to the data object" (claim 26)	"combines/combining the e-mail message [or data object], a new distribution list, and a rule history into a wrapped message" "*rule history*": "a list identifying each of the [or at least one] business rule[s] whose antecedent condition was satisfied by the e-mail message [or data object]"	"Affixes/Affixing to the e-mail message (1) address information for at least one new destination post office for receiving the e-mail message for review by an administrator associated with the destination post office, (2) information identifying the reasons [or at least one reason] why the e-mail message was designated for administrator review by at least one rule engine"